

Software Development Lifecycle Vulnerabilities Checklist

Area	Procedures	Status	Notes
Controls over data handling.	<ul style="list-style-type: none"> - Are inventories kept up-to-date? - Is there an inventory for physical media, especially those that may contain sensitive corporate data? - Can an authorized user simply put a diskette in his or her pocket and walk out of the building? - How is paper eliminated from the office space? - Are shredders used to make removal of sensitive documents from trash cans more difficult? 		
Weak or missing physical controls.	<ul style="list-style-type: none"> - Are key elements of a network located in a shared location? - Does the organization require employee identification badges to be worn? - Are they trained to question the person or bring his or her presence to someone's attention? 		
Inadequate procedural controls.	<p>Clear, concise, written procedures can help to eliminate confusion over specific processes and to ensure that management security objectives are implemented. They can also help to fill voids when trained personnel leave the company or move to other positions. The problem is that many people do not like to write down procedures, and many descriptions are written without the procedures being fully implemented.</p>		
Poor programming practices.	<p>For years the practice of writing backdoors into software programs to enable programmers to enter and fix problems later has been followed. This practice creates two major problems. First, programmers sometimes forget to remove these backdoors prior to code being shipped. Second, backdoors are an avenue that many would-be attackers search for and like to use to gain unauthorized access to systems. Software programs need to be written with security as part of the foundation, which includes the use of sound programming practices.</p>		
Operating system weaknesses.	<p>The biggest security challenge for most system administrators is keeping up with the latest patches for operating systems. This is a real challenge for software vendors as well, because resource-sharing functions typically contradict the security requirements. Therefore, a tradeoff is typically made to try and balance the two. Operating systems need to be hardened before being placed on production systems. Once they become operational, system administrators need to remain vigilant, watching for new vulnerabilities and patches as they may be discovered. Teamwork between system administrators, the security community, and vendors is the best way to guard against operating system weaknesses.</p>		